



UNITED STATES PATENT AND TRADEMARK OFFICE

49

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,808	05/15/2001	Gerald R. Malan	UOM0234PUS	1533

7590 , 12/06/2005
David R. Syrowik
Brooks & Kushman P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1351

EXAMINER

FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/855,808
Filing Date: May 15, 2001
Appellant(s): MALAN ET AL.

MAILED

DEC 06 2005

Technology Center 2100

David R. Syrowik, Reg. No. 27,956
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9/19/05 appealing from the Office action mailed 5/5/05.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Application Serial No. 09/855,810 for: "Method and System for Reconstructing a Path Taken By Undesirable Network Traffic".

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-19, 21-23 and 26-33 are rejected under 35 U.S.C. 102 as being anticipated by Belissent. This rejection is set forth in the prior Office action dated 5/5/05 and repeated here for convenience.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-19, 21-23, and 26-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Belissent (US Patent No. 6,789,203).

Regarding claim 1, Belissent teaches a system for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising:

a collector adapted to receive a plurality of data statistics from the computer network and to process the plurality of data statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies (col.5 lines 45-56), and

a controller coupled to the collector to receive the signal (col.6 lines 2-17:

throttler unit 216) ;

wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source, and wherein the controller is constructed and arranged to block the one or more data packet flow anomalies (col.6 lines 2-17: throttler unit 216).

Regarding claim 2, Belissent teaches the collector includes a buffer coupled to the computer network and being adapted to process the plurality of data statistics to generate at least one record (col.5 lines 36-51).

Regarding claim 3, Belissent teaches the collector further includes a profiler coupled to the buffer and being adapted to receive and process the record to generate a predetermined threshold (col.5 line 48 thru col.6 line 17).

Regarding claim 4, Belissent teaches the profiler includes means for aggregating the data statistics to obtain a traffic profile of network flows (col.5 line 48 thru col.6 line 17).

Regarding claim 5, Belissent teaches the data statistics are aggregated base on at least one invariant feature of the network flows (col.5 line 48 thru col.6 line 17).

Regarding claim 6, Belissent teaches data statistics are aggregated based on temporal, statistic network and dynamic routing parameters (col.5 line 48 thru col.6 line 17).

Regarding claim 7, Belissent teaches the at least one invariant feature includes source and destination endpoints (col.5 line 48 thru col.6 line 17).

Regarding claim 8, Belissent teaches the collector further includes a detector

coupled to the buffer and to the profiler, the collector being adapted to receive and process the record and the predetermined threshold to detect if attributes associated with the record exceed the predetermined threshold representing the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17).

Regarding claim 9, Belissent teaches the collector further includes a local controller coupled to the detector and to the profiler and being adapted to receive and respond to the one or more data packet flow anomalies by generating the signal representing the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17).

Regarding claim 10, Belissent teaches the detector includes a database for storing the at least one record, predetermined threshold, the one or more data packet flow anomalies, and related information (col.5 lines 56-61).

Regarding claim 11, Belissent teaches the profiler includes a database for storing a plurality of data packet flow profiles and related information (col.5 lines 56-61).

Regarding claim 12, Belissent teaches the controller includes a filtering mechanism for blocking the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17, col.6 lines 26-40).

Regarding claim 13, Belissent teaches the filtering mechanism includes a plurality of filter list entries (col.5 line 48 thru col.6 line 17, col.6 lines 26-40).

Regarding claim 14, Belissent teaches the filtering mechanism includes a plurality of rate limiting entries (col.5 line 48 thru col.6 line 17-, col.6 lines 26-40).

Regarding claim 15, Belissent teaches the controller includes a correlator

coupled to the collector and being adapted to receive and normalize the plurality of signals representing the one or more data packet flow anomalies and to generate an anomaly table including the attributes related to the one or more data packet flow anomalies (col.5 line 48 thru col.6 line 17; col.6 lines 41-44).

Regarding claim 16, Belissent teaches the correlator includes a database for storing the anomaly table (col.5 lines 56-61, col.6 lines 41-44).

Regarding claim 17, Belissent teaches the correlator further includes an adapter that is constructed and arranged to communicate the anomaly table to a computing device for further processing (col.5 lines 56-61).

Regarding claim 18, Belissent teaches the controller further includes. :
a web server (col.5 lines 6-9), and
access scripts that cooperate with the web server to enable the access the database defined on the controller to view the computing device to anomaly table (col.5 line 56 thru col.6 line 17).

Regarding claim 19, Belissent teaches a system comprising:
at least one routing system (col.5 lines 42-56),
a plurality of computer systems coupled to the routing system, and means for detecting one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system (col.1 lines 46-51, col.5 lines 4-9, col.5 line 48 thru col.6 line 17).

Regarding claim 21, Belissent teaches a means for blocking the one or more denial of service attacks communicated to the plurality of computer systems over the at

least one routing system (col.5 line 34 thru col.6 line 17).

Regarding claim 22, Belissent teaches means for detecting includes a means for collecting a plurality of data statistics from the at least one routing system (col.5 line 34 thru col.6 line 17).

Regarding claim 23, Belissent teaches the means for detecting further includes a means for processing the plurality of data statistics to detect one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 26, Belissent teaches a means for communicating the one or more denial of service attacks to a computing device for further processing (col.5 line 34 thru col.6 line 17).

Regarding claim 27, Belissent teaches a method for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising the steps of:

collecting a plurality of data statistics from the computer network (col.5 lines 21-55)

processing the plurality of data statistics to detect one or more data packet flow anomalies (col.5 lines 56-61)

generating a plurality of signals representing the one or more data packet flow anomalies (col.5 lines 62-67 thru col.6 lines 1-10) and

receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source (col. 5 lines 56 thru col.6 lines 11-17)

Regarding claim 28, Belissent teaches the step of blocking the one or more data packet flow anomalies in close proximity to the at least one source (col.5 line 34 thru col.6 line 17).

Regarding claim 29, Belissent teaches the step of collecting the plurality of data statistics includes:

buffering the plurality of data statistics,
processing the plurality of data statistics to generate at least one record', and
receiving and profiling the at least one record to generate a predetermined threshold (col.5 line 34 thru col.6 line 17).

Regarding claim 30, Belissent teaches the step of collecting the plurality of data statistics further includes:

detecting if attributes related to the at least one record exceed the predetermined threshold representing the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 31, Belissent teaches the step of collecting the plurality of data statistics further includes:

responding locally to the one or more data packet flow anomalies by generating the plurality of signals representing the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 32, Belissent teaches the step of receiving and responding to the plurality of signals includes:

correlating the plurality of signals representing the one or more data packet flow

anomalies, and

generating an anomaly table including the attributes related to the one or more data packet flow anomalies (col.5 line 34 thru col.6 line 17).

Regarding claim 33, Belissent teaches the step of receiving and responding to the plurality of signals further includes the step of communicating the anomaly table to a computing device for further processing (col.5 line 34 thru col.6 line 17).

(10) Response to Argument

In general, the appellant's arguments fail to consider the full teachings of the reference in light of the knowledge generally available to one of ordinary skill in the art.

Appellant argues Belissent fails to disclose the generation of one or more signals or alert message representing anomalies based on processed packet flow statistics which signal (s) is responded to by tracking or tracing attributes related to the anomalies to a source or origin of the attacks. Belissent discloses a system for preventing a denial of service attack over a computer network, by using an IP throttler. The IP throttler prevents denial of service attacks, records all connecting IP addresses, and allows the network server to detect attackers as shown in Column 4, lines 9-20. As shown in Column 5, lines 21-55, each data packet routed over a network contains an IP address associated with the client's computer. The IP address is a means for data packet flow statistics. The client's computer has an IP address associated with it, allowing the client to request a connection to the server. The throttler collects a plurality of IP addresses routed from a server to the computer network. The throttler processes the plurality of IP addresses to detect one or more data packet flow anomalies. The threshold values and

the number of connection requests are means for data packet flow anomalies. Also, Belissent discloses in Column 5, lines 56-61, the data packet flow anomalies (i.e., predetermined threshold values and IP address) are stored within the memory and used to determine if the client is characterized as an attacker. By storing the threshold values and IP address, the client's IP address which is the source address is used as a tracking attribute for detecting an attacker. Therefore, one or more signals are generated by the throttler unit if the client's connection request rate exceeds the predetermined threshold values as shown in Column 5, lines 62-67, Column 6, lines 1-10. After receiving the signal, the throttler unit responds by tracking the IP address (tracking attributes) related to the data packet flow anomaly (threshold value) to the source (attacker) and rejecting new connection requests from the offending requestor (source) as shown in Column 6, lines 11-17. Furthermore, Belissent discloses the feature of tracking by to the source, by storing the IP address and the threshold values within the memory of the processor unit. This determines whether or not the client is characterized as the attacker and it allows the server computer to track back to the original source associated with the IP address of the client's computer as shown in Column 5, lines 56-61.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,


Application/Control Number: 09/855,808
Art Unit: 2137

Page 11


Courtney D. Fields

November 22, 2005

Conferees:

Kim Vu 

Emmanuel Moise 